



CITY OF ATLANTA


LESLIE WARD
City Auditor
lward1@atlantaga.gov

AMANDA NOBLE
Deputy City Auditor
anoble@atlantaga.gov

CITY AUDITOR'S OFFICE
68 MITCHELL STREET SW, SUITE 12100
ATLANTA, GEORGIA 30303-0312
(404) 330-6452
FAX: (404) 658-6077

AUDIT COMMITTEE
Fred Williams, CPA, Chair
Donald T. Penovi, CPA, Vice Chair
Marion Cameron, CPA
C.O. Hollis, Jr., CPA, CIA
Ex-Officio: Mayor Kasim Reed

TO: Honorable Mayor and Members of the City Council

FROM: Leslie Ward 

DATE: May 22, 2012

SUBJECT: Implementation of Audit Recommendations: Department of Information Technology

We undertook this audit to assess the extent to which city officials have taken timely, appropriate corrective action in response to audit findings and recommendations. The city charter requires my office to report on completed audits, major findings, management's corrective actions, and significant findings that have not been fully addressed.

We followed up on 20 recommendations related to information technology from four audits: *Police Computer Aided Dispatch Data Reliability* (April 2008), *Aviation Terminal Leases* (August 2009), *Water Customer Information Systems* (December 2009) and *Information Technology General Controls* (November 2010). The recommendations range in age from 13 to 48 months old. Management agreed with all 20 of the recommendations and planned to implement most within a few months. Since we made the recommendations, the city has consolidated information technology functions from the departments of Aviation and Watershed Management into the Department of Information Technology. We conducted this audit in accordance with generally accepted government auditing standards. Our audit methods included:

- obtaining management's assessment of whether each recommendation has been implemented, partially implemented, or not implemented
- reviewing departments' responses and data submissions to understand how management addressed each audit recommendation
- examining documentation for a judgmental sample of system changes to determine whether management followed its defined controls

- Testing and analyzing data to confirm management’s assessment of the implementation status of the recommendations, including:
 - examining the application user accounts to identify whether terminated users maintain access
 - examining the settings applied to application users account to determine whether they adhere to the established password policy
 - examining system settings to determine whether they help to prevent the risk of unauthorized access.
- Reviewing application reports to determine whether they deliver the required functionality.

City staff has implemented three and partially implemented seven of the 20 recommendations we followed up in this report. Two of the 20 recommendations are no longer relevant in light of the city’s information technology consolidation. The remaining eight recommendations have yet to be implemented. We reassigned one recommendation issued to the Department of Information Technology to the Department of Law. We also consolidated three change management recommendations into one recommendation for future follow up. Appendix A summarizes our assessment of each recommendation.

City systems continue to be at risk for unauthorized access. The combination of failure to close unused accounts, lack of review on Oracle security logs, weak passwords, and unrestricted vendor access to enQuesta increase the likelihood of unauthorized access and misuse of sensitive data.

- 60 terminated or retired employees still had access to the Oracle Financials application
- 3 terminated employees out of a sample of 25 users still had access to the enQuesta application
- 2,034 Oracle accounts failed to comply with established password settings; 11 of these accounts belonged to city employees, the remainder were vendor accounts
- 293 enQuesta accounts failed to comply with established password settings
- No one reviews Oracle security logs to identify unusual activities
- Vendor access to enQuesta remains unrestricted and unmonitored; the vendor is able to remotely access the system using the most powerful operating system account

Change management continues to pose risk. Staff did not consistently document the testing, approval, and review of changes to the Oracle Financials application. According to city policy, each scheduled change must be approved by functional owners prior to development, tested by the user population, approved for migration into the production environment by the change control board, and reviewed after implementation to certify the change functioned as intended. Failure to follow the established change control policies increases the risk of system destabilization or other unintended consequences.

Time keeping continues to pose risk. The Department of Information Technology developed a report that compares time entries recorded in Kronos to time paid in Oracle. This comparison is limited to differences in pay code, such as regular pay, sick leave and overtime pay. As such, the report lacks the details necessary for payroll staff to identify which employees have been overpaid or underpaid. Payroll staff examines the report to determine whether the difference is at a level they deem acceptable. The city overpaid employees a total of 183 hours for the pay period ending September 28, 2011. The Director of payroll told us the department has not used the report to make any pay adjustments. Overpayment to employees was first identified as an issue in our audit of the first payroll run released in April 2008.

The city continues to be vulnerable to prolonged service interruptions. The Department of Information Technology still lacks business continuity and disaster recovery plans for critical city systems. Planning for disasters and testing to determine if the plan works can reduce costs and time needed to restore critical services. Also, the department has yet to establish service level agreements with the departments it serves. Service level agreements are a key control for defining and managing services that meet business needs. The department identified continuity of operations as a strategic imperative and service level agreements as an element of improving IT delivery service in its fiscal year 2011 strategic plan. The strategic plan also included an analysis of the department's staffing needs, which reports a staffing shortage of 85 employees. However, the department overstated its unmet staffing need by failing to include contractors in its analysis. We recommended the department include contractor support in its calculation of staffing needs in our IT General Controls audit released in November 2010.

Watershed Management billing and collection system requirements are still unmet. In response to the *Water Customer Information Systems* audit, the Department of Watershed Management acknowledged that its vendor had yet to fulfill four functional requirements related to billing and collections reports. While management said it expected the vendor to meet these requirements, the system still does not: generate a roll-forward of receivables at certain time periods, calculate the current collection rate, or produce aging reports showing delinquencies of 120 days or 1-4 years and greater. These features were all required under watershed management's implementation agreement and were consistent with our previous audit recommendations. Staff manually creates the roll-forward reports. Neither staff nor the application can calculate or report the current collection rate.

The three implemented recommendations deal with the Police Department's computer aided dispatch system and the Department of Watershed Management's billing system. The Department of Information Technology and Northrop Grumman, the contractor responsible for operating the Police Department's computer aided dispatch system, resolved a problem that had resulted in gaps in recorded incident numbers, first reported in our 2008 performance audit, *Police Computer Aided Dispatch Data Reliability*. Northrop Grumman determined that the gaps occurred when data entered during staff training were deleted. Northrop Grumman created a separate version of the dispatch system for training to isolate training from live records. The Department of Watershed Management evaluated and documented business reasons for deciding not to implement three of seven system

requirements that had not been met when we conducted a post-implementation review of enQuesta released in December 2009. The department has also developed in-house expertise to extract and analyze data from enQuesta, which should allow the department to make better use of its data to support management decisions and to respond to stakeholder requests for information.

Generally accepted government auditing standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The Audit Committee has reviewed this report and is releasing it in accordance with Article 2, Chapter 6 of the City Charter. We appreciate the courtesy and cooperation of city staff throughout the audit. The team for this project was Damien Berahzer and Lesia Johnson.

Cc: Duriya Farooqui, Interim Chief Operating Officer
Michael Dogan, Interim Chief Information Officer
Dennis Rose, Deputy Chief Information Officer
Daphne Rackley, Deputy Chief Information Officer
Jaci Vickers, ERP Director
Rhonda Johnson, Municipal Clerk

Attachment A:

Audit Recommendations Remaining Open

	Report Title and Date	Recommendation	City Auditor Analysis	Implementation Status
1	<p>Information Technology Controls November 2010</p> <p>Management Agreed</p> <p>Expected Implementation Date: November 2010</p>	<p>The chief information officer should update the department's strategic plan to reflect the city's current needs.</p>	<p>The chief information officer updated the department's strategic plan but failed to account for contractors in the analysis of staffing needs.</p>	<p>Partially Implemented</p>
		<p>Updated Management Response: <i>The framework for the Strategic Plan has been developed; however, additional work is needed to develop and prioritize DIT Objectives, Measurements and Tactics.</i></p> <p>Updated Implementation Date: <i>February 2013</i></p> <p>Responsible Person: <i>Michael Dogan</i></p>		
	Report Title and Date	Recommendation	City Auditor Analysis	Implementation Status
2	<p>Information Technology Controls November 2010</p> <p>Management Agreed</p> <p>Expected Implementation Date: TBD</p>	<p>The chief information officer should work with departments to establish service level agreements consistent with the department's updated strategic plan.</p>	<p>The chief information officer has not established service level agreements consistent with the department's strategic plan.</p>	<p>Not Implemented</p>
		<p>Updated Management Response: <i>The SLAs will be re-evaluated with the completion of the Strategic Plan</i></p> <p>Updated Implementation Date: <i>TBD</i></p> <p>Responsible Person: <i>Michael Dogan</i></p>		

	Report Title and Date	Recommendation	City Auditor Analysis	Implementation Status
3	Information Technology Controls November 2010 Management Agreed Expected Implementation Date: TBD	The chief information officer should evaluate options and seek funding to develop business continuity and disaster recovery plans for the city.	The chief information officer has identified business continuity and disaster recovery as strategic imperatives and plans to seek funding to develop business continuity and disaster recovery plans in fiscal year 2013.	Not Implemented
<p>Updated Management Response: Multiple budgetary requests have been submitted, including FY13; however, approval was not granted.</p> <p>Updated Implementation Date: TBD Responsible Person: Michael Dogan</p>				
	Report Title and Date	Recommendation	City Auditor Analysis	Implementation Status
4	Information Technology Controls November 2010 Management Agreed Expected Implementation Date: TBD	The chief information officer should work with the commissioner of human resources to ensure the department is notified when employees leave city employment to enable prompt removal of user access to city systems.	Terminated employees continue to maintain access to city systems. At least 60 former employees retained access to the Oracle Financials application. The department periodically reviews users for the Oracle Financials application. This review identifies separated employees that maintained access subsequent to their departure.	Partially Implemented
<p>Updated Management Response: We will continue to work with DHR to develop a process that encompasses the capture of data related to employees that are no longer with the city, but also to include employees that are moving to other job functions.</p> <p>Updated Implementation Date: September 2012 Responsible Person: Michael Dogan</p>				

	Report Title and Date	Recommendation	City Auditor Analysis	Implementation Status
5	<p>Department of Watershed Management Customer Information Systems December 2009</p> <p>Management Agreed</p> <p>Expected Implementation Date: December 2009</p>	<p>Determine why some system requirements were not implemented and whether the vendor can be held accountable for implementing them now.</p>	<p>The Department of Watershed Management failed to hold the vendor accountable for the implementing four system requirements:</p> <ul style="list-style-type: none"> • The enQuesta Water CIS application provides the ability to generate a roll-forward of receivables one year old, two years old, three years old, four years old and years greater indicating the beginning balance, adjustments, payments and ending balance by each year in order to compute the allowance for doubtful account and/or bad debt ratio. • The enQuesta Water CIS application provides the ability to generate a monthly roll-forward of total receivables indicating the beginning balance, adjustments, payments and ending balance • The enQuesta CIS application provides the ability to provide an aging report by 30 days, 60 days, 90 days, one year, two years, three years, four years and amounts greater than four years. • The enQuesta CIS application provides a computation of the billing versus collection rate separating current billings / current collections and also total billings/total collections, which includes prior year calculations. The application also provides this information by class of customer i.e. residential, commercial, industrial, and institutional. 	<p>Not Implemented</p>

	Report Title and Date	Recommendation	City Auditor Analysis	Implementation Status
		<p>Updated Management Response: <i>While the capability and methodology to develop the A/R and Collection Rates was verified within enQuesta, the actual reports were not available during the auditor's review period, but are now available.</i></p> <p>Updated Implementation Date: <i>Completed April 2012</i></p> <p>Responsible Person: <i>Daphne Rackley</i></p>		
	Report Title and Date	Recommendation	City Auditor Analysis	Implementation Status
6	<p>Department of Watershed Management Customer Information Systems December 2009</p> <p>Management Agreed</p> <p>Expected Implementation Date: December 2009</p>	<p>Ensure that watershed management staff reviews all user accounts (with the exception of the root account) and enforce the established password policies.</p>	<p>User accounts continue to have password settings that are weaker than the established password policies. We identified:</p> <ul style="list-style-type: none"> • 293 accounts do not follow the minimum password settings • 7 accounts can reuse existing passwords and • 3 accounts whose passwords does not expire • All accounts lock after three invalid login attempts 	<p>Partially Implemented</p>
		<p>Updated Management Response: <i>We will investigate and identify why the password setting criteria is not being applied consistently and rectify.</i></p> <p>Updated Implementation Date: <i>May 2012</i></p> <p>Responsible Person: <i>Daphne Rackley</i></p>		

	Report Title and Date	Recommendation	City Auditor Analysis	Implementation Status
7	<p>Department of Watershed Management Customer Information Systems December 2009</p> <p>Management Agreed</p> <p>Expected Implementation Date: March 2010</p>	<p>Ensure that watershed management staff review all user accounts in enQuesta and the UNIX operating system and remove IDs belonging to terminated users and generic IDs that are no longer needed.</p> <p>Updated Management Response: <i>As part of a larger issue with removing IDs for terminated employees or employees that have moved to other functions and no longer need access to the system, we are continuing to work with DHR to develop a comprehensive and reliable method of notification and a process within DIT to ensure that each relevant application is updated appropriately.</i></p> <p>Updated Implementation Date: September 2012</p>	<p>Terminated employees continue to maintain access to city systems. At least four former employees retained access to enQuesta after they no longer worked for the department, including one account that we identified in the 2009 audit.</p> <p>Responsible Person: Daphne Rackley</p>	<p>Not Implemented</p>
	Report Title and Date	Recommendation	City Auditor Analysis	Implementation Status
8	<p>Department of Watershed Management Customer Information Systems December 2009</p> <p>Management Agreed</p> <p>Expected Implementation Date: December 2009</p>	<p>Enforce system settings to limit remote logon using the root account.</p> <p>Updated Management Response: <i>We will set up a policy for accessing enQuesta which will entail setting up administrative groups with permissions based on roles. If the vendor requires root access for any reason they would have to get it from the Security team and then the root password would be changed as soon as they have completed the task. We anticipate root level access to be an infrequent need.</i></p> <p>Updated Implementation Date: June 2012</p>	<p>The department prevented the root account from using the file transfer protocol but failed to limit other remote login protocols for this account.</p> <p>Responsible Person: Daphne Rackley</p>	<p>Partially Implemented</p>

	Report Title and Date	Recommendation	City Auditor Analysis	Implementation Status
9	<p>Department of Watershed Management Customer Information Systems December 2009</p> <p>Management Agreed</p> <p>Expected Implementation Date: March 2010</p>	<p>Establish a policy that governs the periodic review and recertification of users for the enQuesta application and removal of terminated users.</p>	<p>The department has not developed a policy to govern periodic review and recertification of users. The department created a committee to oversee this function, but the committee had not reviewed application users as of February 2012]. The department said the committee would review users in collaboration with the vendor within a couple months.</p>	Not Implemented
		<p>Updated Management Response: <i>The CIS Committee is charged with this task; however, due to the senior management changes that are still in transition for the billing/customer service bureau, the committee has not been able to complete this task, but will resume when key senior leadership personnel have been identified. However, the removal of terminated users is not dependent upon this and is a part of open recommendation 7.</i></p> <p>Updated Implementation Date: TBD</p> <p>Responsible Person: Daphne Rackley</p>		
	Report Title and Date	Recommendation	City Auditor Analysis	Implementation Status
10	<p>Department of Watershed Management Customer Information Systems December 2009</p> <p>Management Agreed</p> <p>Expected Implementation Date: March 2010</p>	<p>Establish a policy that limits vendor access to the production instance of enQuesta to an as-needed basis and governs how, when, and who is responsible for granting the vendor system access, and consider monitoring what is done by the vendor.</p>	<p>The Department of Watershed Management continues to grant the vendor 24/7 administrative access to the enQuesta application. The department has apparently misinterpreted a requirement for broadband access to mean 24/7 access. The department said it plans to implement monitoring software to track the vendor's activities on enQuesta.</p>	Not Implemented
		<p>Updated Management Response: <i>We do have the ability to monitor what is done by the vendor and the process is for the vendor to contact IT before making any changes to the system; however, as the city takes a stronger role in administering the system, the reliance on vendor support is decreasing. With that, we are evaluating the process of providing vpn only when needed.</i></p> <p>Updated Implementation Date: June 2012</p> <p>Responsible Person: Daphne Rackley</p>		

Attachment B: Audit Recommendations Closed

	Report Title and Date	Recommendation	City Auditor Analysis	Implementation Status
1	<p><i>Police Computer Aided Dispatch Data Reliability</i> April 2008</p> <p>Management Agreed</p> <p>Expected Implementation Date: March 2008</p>	<p>The Chief Information Officer should direct Northrop Grumman to investigate why there are gaps in incident numbers, determine whether records are missing, and if so whether system or operating changes are necessary to resolve the problem.</p>	<p>Northrop Grumman determined that the gap in incident numbers resulted from deleting fictitious dispatch records created during training. The contractor has implemented a test environment to support training without affecting the dispatch system.</p>	<p>Implemented</p>
2	<p><i>Airport Terminal Leases</i> August 2009</p> <p>Management Agreed</p> <p>Expected Implementation Date: August 2009</p>	<p>The Department of Information Technology should involve key stakeholders and application owners early in the [change management] process in order to provide time for meaningful analysis of options and identify risk to the system to address future problems with the system.</p>	<p>The Department of Information Technology did not document inclusion of key stakeholders for one of two Oracle Financials system changes we sampled.</p>	<p>Closed</p> <p>Recommendation Replaced by New Recommendation #2 in Appendix C</p>
3	<p><i>Information Technology Controls</i> November 2010</p> <p>Management Agreed</p> <p>Expected Implementation Date: November 2010</p>	<p>The chief information officer should update department policies to strengthen security and to reflect actual practices.</p> <ul style="list-style-type: none"> • documenting procedures regarding sequencing and scheduling jobs • ensuring the backup policy reflects its current contract • regularly test its ability to restore data • periodically reviewing security logs • periodically reviewing and validating the list of employees with access to 	<p>According to Department of Information Technology staff, job sequencing and scheduling follows established change control processes. The change in job scheduling that we sampled showed no evidence that staff tested the change before implementation or reviewed it after migration to production.</p> <p>We confirmed that the department is shipping backup tapes off site in accordance with its policy and is regularly</p>	<p>Closed</p> <p>Recommendation Replaced by New Recommendation #1 and Recommendation #2 in Appendix C</p>

	Report Title and Date	Recommendation	City Auditor Analysis	Implementation Status
		<p>each city system</p> <ul style="list-style-type: none"> strengthening password policies applicable to Oracle 	<p>testing its ability to restore backed up data.</p> <p>The department also developed a policy for reviewing security logs, but has yet to implement the policy</p> <p>The department has implemented a periodic review of users for the Oracle Financials application.</p> <p>The department applied password settings in accordance with city policy to most Oracle accounts. However, we identified 2,034 with no password expiration setting applied. We also found that a few Department of Information Technology personnel overrode established password settings on their own accounts.</p>	
4	<p>Information Technology Controls November 2010</p> <p>Management Agreed</p> <p>Expected Implementation Date: November 2010</p>	<p>The chief information officer should ensure that approval for system changes is documented prior to implementation.</p>	<p>While all three system changes we reviewed showed evidence of the Change Control Board's approval, the department did not document approval from stakeholders</p> <ul style="list-style-type: none"> approved by functional owners prior to development, tested by the user population 	<p>Closed Recommendation Replaced by New Recommendation #2 in Appendix C</p>
5	<p>Information Technology Controls November 2010</p> <p>Management Agreed</p>	<p>The chief information officer should work with the city attorney to identify laws and regulations that apply to city data and develop procedures to classify and protect data commensurate with requirements.</p>	<p>The chief information officer requested assistance from the Department of Law, which initially responded that the request was too broad.</p>	<p>Closed Recommendation Reassigned to the Department of Law in New</p>

	Report Title and Date	Recommendation	City Auditor Analysis	Implementation Status
	Expected Implementation Date: TBD			Recommendation #3
6	<p>Information Technology Controls November 2010</p> <p>Management Agreed</p> <p>Expected Implementation Date: TBD</p>	The chief information officer should work with the controller to establish a process to reconcile differences between Kronos and Oracle.	The Department of Information Technology developed a report to flag net differences in amounts paid by pay code between Oracle and Kronos each pay period, but the report lacks the detail necessary for the payroll group to identify and correct individual errors. The payroll department has not used the report to make any pay adjustments.	<p>Closed</p> <p>Recommendation Replaced by New Recommendation #4 in Appendix C</p>
7	<p>Department of Watershed Management Customer Information Systems December 2009</p> <p>Management Agreed</p> <p>Expected Implementation Date: December 2009</p>	Document business reasons for choosing not to implement some requirements.	<p>The Department of Watershed Management documented the business reasons for not implementing three system requirements:</p> <ul style="list-style-type: none"> • Customers are enabled to apply for service via the internet. • The enQuesta application provides the ability to link accounts for the purpose of generating a single bill to a master account. • The enQuesta application provides the ability to request budget billing via the World Wide Web/Internet 	Implemented
8	<p>Department of Watershed Management Customer Information Systems December 2009</p> <p>Management Agreed</p> <p>Expected Implementation Date: December 2009</p>	Develop in-house expertise on the extraction and analysis of data from the enQuesta application.	Department of Watershed Management staff is able to extract and analyze enQuesta data and has created reports to support operations.	Implemented

	Report Title and Date	Recommendation	City Auditor Analysis	Implementation Status
9	<p>Department of Watershed Management Customer Information Systems December 2009</p> <p>Management Agreed</p> <p>Expected Implementation Date: June 2010</p>	Develop departmental expertise in the areas of system security and IT governance, or establish a relationship with the city's Department of Information Technology.	As part of the city's information technology consolidation, the Department of Watershed Management IT function reports to the chief information officer. The Department of Information Technology is responsible for system security and IT governance.	<p>Closed</p> <p>No Longer Relevant</p>
10	<p>Department of Watershed Management Customer Information Systems December 2009</p> <p>Management Agreed</p> <p>Expected Implementation Date: March 2010</p>	Establish a formal change control policy that governs watershed management's areas of responsibility for changes to the enQuesta application.	As part of the city's information technology consolidation, the Department of Information Technology change control policy covers changes to enQuesta	<p>Closed</p> <p>No Longer Relevant</p>

Attachment C: New and Reassigned Recommendations

1. The chief information officer should enforce the established policies to strengthen security and to reflect actual practices in order to clarify expectations of staff and ensure consistency. Measures should be developed to identify when the following controls are not enforced :
 - periodically reviewing security logs
 - applying the established password settings for the Oracle Financials application user base
2. The chief information officer should ensure that the controls established to ensure the integrity of system changes are followed by IT personnel. These controls include documenting:
 1. request for changes
 2. authorization of the change by the functional/owner base
 3. user testing verifying the change worked as intended
 4. approval to migrate the change into the production environment
 5. review by DBA to ensure all documentation is available prior to moving into production
 6. post implementation assessment the change to ensure it had the desired effect and no subsequent issues have developed
3. The City Attorney should identify laws and regulations that apply to city data. The review of laws and regulations performed should include, but not limited to:
 1. PCI (Payment Card Industry) Standards
 2. HIPPA (Health Insurance Portability and Accountability Act)
 3. FISMA (Federal Information Security Management Act)
4. The chief information officer should develop reports showing variances between Kronos and Oracle. These reports should contain details for each employee having an amount paid in Oracle different to what is recorded in Kronos.

Attachment D: Management Review and Response to Audit Recommendations

Report # 11.09A	<u>Report Title:</u> Implementation of Audit Recommendations: Department of Information Technology	3/16/2012
Recommendation # 1	Degree of Agreement	
<p>The chief information officer should enforce the established policies to strengthen security and to reflect actual practices in order to clarify expectations of staff and ensure consistency. Measures should be developed to indentify when the following controls are not enforced :</p> <ul style="list-style-type: none"> • periodically reviewing security logs • applying the established password settings for the Oracle Financials application user base 	Agree	
	Implementation Timeframe	
	Security Logs - June 1, 2012	
	Password - complete	
Responsible Person		
1 - Dirk Stewart 2 - Jaci Vickers		
<p><u>Proposed Action:</u></p> <ol style="list-style-type: none"> 1. <u>Periodically reviewing security logs:</u> The Chief Security Officer will begin periodic review of the security logs (every month); ERP Program Director will assist with needed reminders. 2. <u>Strengthening password policies applicable to Oracle:</u> On April 3, 2011, we forced all existing employee and vendor accounts to have following settings: <ul style="list-style-type: none"> • Change their Oracle password every 60 days. • Must wait 180 days to reuse a password. • Have their access revoked after 5 unsuccessful attempts to log on. • Have their password adhere to the following standards: <ol style="list-style-type: none"> a. Must contain at least one letter and at least one number. b. Cannot contain the user name or repeating characters. c. Must be at least 8 characters in length. d. Characters can be upper or lower case. <p style="text-align: right;">However, due to the nature of how we set up accounts created subsequent to April 3, 2012, some</p>		

accounts did not adhere to the password expiration of 60 days. A concurrent program was created and installed that is run weekly to default ALL Oracle user records with no expiration date to reset their passwords every 60 days.

Recommendation # 2	Degree of Agreement
<p>The chief information officer should ensure that the controls established to ensure the integrity of system changes are followed by IT personnel. These controls include documenting:</p> <ol style="list-style-type: none"> 1. request for changes 2. authorization of the change by the functional/owner base 3. user testing verifying the change worked as intended 4. approval to migrate the change into the production environment 5. review by DBA to ensure all documentation is available prior to moving into production 6. post implementation assessment the change to ensure it had the desired effect and no subsequent issues have developed 	Agree
	Implementation Timeframe
	May 30, 2012
	Responsible Person
Jaci Vickers	
<p><u>Proposed Action:</u> ERP Program Director will work with functional and technical teams to revise and enforce this policy. Nominally, approval in Remedy/Numera to include updating in the Activity Log will be required.</p>	
Recommendation # 3	Degree of Agreement
<ol style="list-style-type: none"> 1. The City Attorney should identify laws and regulations that apply to city data. The review of laws and regulations performed should include, but not limited to: <ol style="list-style-type: none"> 1. PCI (Payment Card Industry) Standards 2. HIPPA (Health Insurance Portability and Accountability Act) 3. FISMA (Federal Information Security Management Act) 	Agree
	Implementation Timeframe
	August 2012
	Responsible Person
Angela Hinton	

Proposed Action: With respect to the Payment Card Industry Standards, those are not laws and, thus, there is no legal issue on which we could opine but the Law Department can recommend that departments that accept credit card payments assess their payment processing practices to determine if any revision is necessary.

The City Attorney’s office will review the Health Insurance Portability and Accountability Act (“HIPAA”) and Federal Information Security Act (“FISMA”) to determine what obligations those laws may impose on the City. We will then confer with the responsible parties to develop some next steps to assure compliance.

Recommendation # 4

Degree of Agreement

The chief information officer should develop reports showing variances between Kronos and Oracle. These reports should contain details for each employee having hours paid in Oracle different to what is recorded in Kronos.

Agree

Implementation Timeframe

September 1, 2012

Responsible Person

Danny Bryant

Proposed Action: The Department of Information Technology agrees that the ability to reconcile detailed wage data is important to the financial soundness of the City. An immediate solution is unavailable, as Kronos’ role is limited to capturing time and not wage related data and these systems reside on separate database systems.

The common data elements between Kronos and Oracle consist of the hours applied to the various pay groups per employee. In response to a modified recommendation based upon hours, the Department of Information Technology is in the process of implementing the Oracle Business Intelligence Enterprise Edition (OBIEE) solution that can consolidate the disparate data sources across the City allowing for the detailed reconciliation of Oracle and Kronos hours charged by employee. The DIT is currently working with the Payroll to determine the necessary data points for this effort.